using the stored security information to enable the client access to the secured network service without requiring the client to supply the stored security information.

REMARKS

Claims 1-30 were pending in the above-identified application when last examined and were rejected. New claims 31-38 are being added. No new matter is being added by virtue of the new claims 31-38, and claims 1-38 remain pending.

In item 9 (page 3), the Examiner rejected claims 1-30 under 35 U.S.C. § 103(a) as being unpatentable over Vogel (US Pat No 5,815,683) and further in view of Netscape version 2. The examiner indicates in item 10 that claims 1, 15, 29 and 30 have been amended to include the limitation "Thereby enabling the client to access the available services without storing the service communication code and keys at the client." The Examiner then continues in item 11 that "it would have been obvious for one of ordinary skill in the art to store access codes and keys at a play [sic] other than the client... storing user keys and access codes at the user site would be [sic] not be good security practice... storing keys on the user computer allows the user access to other users." Applicant respectfully traverses.

Applicant respectfully submits that the above rejection, which has been repeated by the Examiner, is not only without any substantial basis whatsoever, but is also contradictory. The Examiner continually fails to present even ONE substantial reference within the cited art supporting the obviousness of at least "a keysafe for storing keys, each key for enabling communication between the client and a respective service from the set of available services" or "enabling the client to access the available services without storing the service communication code and keys at the client", as in the embodiment recited by claim 1. Instead, the Examiner apparently relies solely on his own impression of ordinary skill in the art at the time of the invention based on the usefulness of an achieved result.

The Examiner is reminded that the level of skill in the art cannot be relied upon to provide the suggestion to combine references. *Al-Site Corp. v. VSI Int'l, Inc.*, 174 F3d 1308, 50 USPQ2d 1161 (1999). Thus, since Vogel and Netscape fail to teach either of the above-noted claim 1 recitations and also fail to suggest the asserted combination, the COMBINATION of the two references cannot render claim 1 obvious under 35 U.S.C. § 103(a).

Moreover, BOTH of the cited references teach away from the recited embodiment.

The Examiner has already admitted that **Vogel** does not teach a keysafe (5/9/00 Office Action, item 4). Further, the complete **Vogel** "security system" is defined as: an access request applet PROMPTS A CLIENT for client information (col. 4, lines 47-48), the client supplies the information and the applet submits the client-supplied information to an access service program in the facilitator (col. 4, lines 59-60, emphasis added). Utilizing only such protection as taught by **Vogel** is clearly contrary to either of the above-noted claim 1 recitations, and the security related portions of the cited **Netscape** reference also fail to teach or suggest at least the above-noted claim 1 elements.

Further, the Examiner has specifically asserted the Netscape Corp. Navigator product, and **Vogel** also mentions that product (e.g. see Vogel at col. 4, line 18). It should therefore also be noted that Netscape's teachings –not only at the time of the invention, but even TODAY- remain contrary to the above-noted claim 1 elements. The attached Exhibits A and B, for example, were printed from posted Netscape Web pages on 6/1/01: "http://home.netscape.com/ certificate/v1.0/ index. html" and "http://home.netscape.com/security/basics/getperscert.Htmlon". As taught therein, "Once a user has opened a browser and entered a password... the client and a server can each... check each other's certificates" (attached as Exhibit A, first paragraph), wherein "a digital certificate is a software tool that you can install IN YOUR BROWSER" (attached as Exhibit B, first paragraph) (emphasis added).

Still further, Applicant has already submitted evidence that the teachings of Microsoft Corp –Netscape's rival in the browser market- remain contrary to the above-noted claim 1 elements even TODAY, let alone at the time of the invention (see Internet Explorer and Outlook Exhibits submitted on 10/31/00).

Thus, despite the Examiner's contentions that the embodiment recited in claim 1 is obvious, he is unable to produce any evidence in support thereof, the teachings of his own references are contrary and the dominate rivals in the field even TODAY purport that the state of the art teaches away from the recited claim 1 embodiment.

The Examiner instead appears to be applying impermissible hindsight. For example, the specification addresses Applicant's observations that "direct access to systems behind firewalls compromises security" (page 4, line 23 – page 5, line 1). The Examiner similarly notes that storing user keys and access codes at the user site would not be good security practice. The specification provides embodiments including those for handling kiosks (e.g. FIG. 1 and page 7,

lines 17-20), among other embodiments particularly thought not necessarily only applicable to a roaming user. The Examiner similarly notes that "storing keys on the user computer allows the user access to other users". It is appreciated that the Examiner has clearly read at least part of the specification and Applicant's prior arguments, and finds aspects of the claimed embodiment to be useful. The issue, under 103a, however, is whether the invention would be obvious to one of ordinary skill at the time of the invention and without knowledge gleaned from the Applicant's disclosure. (*In Re McLaughlin* 443 F.2d 1392, 1395, 170 USPQ 209, 212 (CCPA 1971) (emphasis added).

For at least the above reasons, withdrawal of the rejections of claim 1 is respectfully solicited.

Claim 15 recites, in part, "enabling the client to access the available services without storing the service communication code and keys at the client." As already noted, BOTH of the cited references not only fail to teach or suggest "enabling the client to access the available services without storing the service communication code and keys at the client", but their teachings are also contrary to at least this element of the claimed embodiment. Further, the publications of the manufacturer corresponding to the **Netscape** reference and its long time rival, Microsoft, are also contrary to at least this element of the claimed embodiment. Rather, the Examiner appears to be supported only by impermissible hindsight.

For at least the above reasons, withdrawal of the rejections of claim 15 is respectfully solicited.

Claim 29 recites, in part, "enabling the client to access the available services without storing the service communication code and keys at the client." As already noted, BOTH of the cited references not only fail to teach or suggest "enabling the client to access the available services without storing the service communication code and keys at the client", but their teachings are also contrary to at least this element of the claimed embodiment. Further, the publications of the manufacturer corresponding to the **Netscape** reference and its long time rival, Microsoft, are also contrary to at least this element of the claimed embodiment. Rather, the Examiner appears to be supported only by impermissible hindsight.

For at least the above reasons, withdrawal of the rejections of claim 29 is respectfully solicited.

Claim 30 recites, in part, "enabling the client to access the available services without storing the service communication code and keys at the client." As already noted, BOTH of the cited references not only fail to teach or suggest "enabling the client to access the available services without storing the service communication code and keys at the client", but their teachings are also contrary to at least this element of the claimed embodiment. Further, the publications of the manufacturer corresponding to the **Netscape** reference and its long time rival, Microsoft, are also contrary to at least this element of the claimed embodiment. Rather, the Examiner appears to be supported only by impermissible hindsight.

For at least the above reasons, withdrawal of the rejections of claim 30 is respectfully solicited.

For at least the above reasons, withdrawal of the rejections of claims 1, 15, 29, and 30 is respectfully solicited. The remaining rejected claims further depend from claims 1, 15, 29, and 30 and are patentable for at least the same reasons that claims 1, 15, 29, and 30 are patentable. Reconsideration of the rejections and early allowance of claims 1-30 is therefore respectfully requested.

Attached hereto are the aforementioned Exhibits A and B.

If the Examiner has any questions or needs any additional information, the Examiner is invited to telephone the undersigned attorney at (650) 843-8796.

If for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. 05-0150.

Respectfully submitted,

Mark D. Riggins

Dated: June 22, 2001

By _____
Marc A. Sockol
Attorney for Applicant
Reg. No. 40,823

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043
Telephone (650) 856-6500
Facsimile (650) 856-3619

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached, enclosed or Exhibits thereof) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to the Commissioner for Patents, Washington, D.C. 20231 on

Date: 06/22/2001 By: _____
Victoria Christopher

Version With Markings To Show Changes Made

In the claims:

The following *NEW* claims were added:

31. A method, comprising:

receiving, as an advance communication, security information corresponding to one or more secured network services;

storing the security information at a remote location from a client;

receiving a client request from the client to access a secured network service; and

using the stored security information to enable the client access to the secured network service without requiring the client to supply the stored security information.

32. A method according to claim 31, wherein the security information is received from the client.

33. A method according to claim 31, wherein the security information includes one or more keys corresponding to respective ones of the secured network services.

34. A method according to claim 31, wherein at least one of the keys includes a certificate for accessing at least one of the secured network services.

35. A method according to claim 31, further comprising determining client privileges of the client, and wherein the using the stored security information is provided if the privileges correspond to privilege requirements of the secured network service.

36. A method according to claim 31, further comprising determining client privileges of the client and enabling the client to select a service from ones of the secured network services corresponding to the determined client privileges.

37. A system, comprising:

means for receiving, as an advance communication, security information corresponding to one or more secured network services;

means for storing the security information at a remote location from a client;

means for receiving a client request from the client to access a secured network service; and

means for using the stored security information to enable the client access to the secured network service without requiring the client to supply the stored security information.

38. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

receiving, as an advance communication, security information corresponding to one or more secured network services;

storing the security information at a remote location from a client;

receiving a client request from the client to access a secured network service; and

using the stored security information to enable the client access to the secured network service without requiring the client to supply the stored security information.